UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/774,720 | 02/09/2004 | Xavier Boyen | ID-5 | 9562 |

36532 7590 11/24/2009

Treyz Law Group
870 Market Street, Suite 984
San Francisco, CA 94102

| EXAMINER | |
|---|---|
| DOAN, TRANG T | |
| ART UNIT | PAPER NUMBER |
| 2431 | |
| MAIL DATE | DELIVERY MODE |
| 11/24/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/774,720 | BOYEN, XAVIER | |
| | Examiner | Art Unit | |
| | TRANG DOAN | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *21 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-12,18 and 19* is/are allowed.

6)☒ Claim(s) *13-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to the amendment filed on 08/21/2009

2. Claims 1-19 are pending for consideration.

### *Response to Arguments*

3. Applicant's argument with respect to the 35 U.S.C. 101 rejection has been fully considered in view of the amendment filed on 08/21/2009, which has been made in record, and the 35 U.S.C. 101 rejection has been withdrawn.

4. Applicant's arguments, filed on 08/21/2009, with respect to claims 1-19 have been fully considered and are persuasive. The rejection of claims 1-19 has been withdrawn.

5. Applicant's arguments with respect to claims 13-17 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh et al. (US 2003/0081785) (hereinafter Boneh) in view of Deng et al. (US 6910129) (hereinafter Deng).

Regarding claim 13, Boneh discloses a method of signing and encrypting a message M comprising: obtaining an identity-based-encryption (IBE) private key of a user (Boneh: paragraph 0049); using the IBE private key to compute, with computing equipment, a commitment to a secret value and a corresponding decommitment (Boneh: paragraphs 0006 and 0017: the public key and the private key in a pair are generated together as the output of a key generation algorithm that takes as input a random seed).

Boneh does not disclose using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment. However, Deng discloses using a symmetric key that is based on the IBE private key to encrypt at least one of the commitment and the decommitment (Deng: column 6, lines 55-57). Therefore, It would have been obvious to a person skilled in the art at the time the invention was made to have included in Boneh the feature of Deng as discussed above for secure communication via an insecure communication channel (Deng: column 3 lines 41-43).

Regarding claim 14, Boneh as modified discloses wherein using the symmetric key to encrypt comprises: concatenating the decommitment and the message (Deng: column 6, lines 55-57; and column 12 lines 19-46); and using the symmetric key to encrypt the concatenated decommitment and message (Deng: column 6, lines 55-57; and column 12 lines 19-46). The same motivation was utilized in claim 13 applied equally well to claim 14.

Regarding claim 15, Boneh as modified discloses wherein using the symmetric key to encrypt comprises: concatenating an IBE public key with the message and the decommitment (Deng: column 12 lines 19-46); and using the symmetric key to encrypt the concatenated IBE public key, decommitment, and message (Deng: column 12 lines 19-46). The same motivation was utilized in claim 13 applied equally well to claim 15.

Regarding claim 16, Boneh as modified discloses wherein computing the decommitment comprises performing multiplication on an elliptic or hyperelliptic curve (Boneh: paragraph 0010).

Regarding claim 17, Boneh as modified discloses comprising computing the symmetric key that is based on the IBE private key by performing a bilinear pairing calculation on an elliptic or hyperelliptic curve (Boneh: paragraphs 0019 and 0040).

***Allowable Subject Matter***

8. Claims 1-12 and 18-19 are allowed.

9. The following is a statement of reasons for the indication of allowable subject matter:

10. Regarding claims 1-12 and 18-19, the prior art does not teach “an identity-based-encryption (IBE) signcryption method in which a sender signs and encrypts a message M for a recipient, comprising: at the sender, digitally signing

and encrypting, with computing equipment, a message M in a signcryption operation using an IBE private key of the sender SKA and an IBE public key of the recipient IDB that is based on the recipient's identity to generate a ciphertext C that is a signed and encrypted version of the message M; sending, with computing equipment, the ciphertext C to the recipient anonymously, wherein an attacker cannot deduce the authorship of the message from the ciphertext C; at the recipient, decrypting, with computing equipment, the ciphertext C using an IBE private key SKB of the recipient that corresponds to the IBE public key IDB, wherein decrypting the ciphertext produces an unencrypted version of the message M and an IBE public key of the sender IDA that corresponds to the IBE private key SKA; and at the recipient or at a third party, after the ciphertext has been decrypted by the recipient, performing, with computing equipment, signature verification in an operation that is separate from the decryption of the ciphertext, wherein performing the signature verification comprises using the decrypted message M and the IBE public key of the sender IDA to prove that the sender signed the message M."

## ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431